# CreateSecurityParameter

O método CreateSecurityParameter permite criar um novo parâmetro de segurança.

Nesta página

* [Uso](#Uso)
* [Amostra](#Amostra)

## Uso

**Privilégios.** Este método requer privilégios de criação.

**Parâmetros.**

A tabela a seguir descreve os parâmetros do método CreateSecurityParameter.

| Parâmetro | Tipo de dados | Valor |
| --- | --- | --- |
| sessionToken | String | sessionToken válido retornado pelo método [general.CreateUserSession](createusersession.htm). |
| name | String | Nome do parâmetro de segurança. |
| descrição | String | Descrição do parâmetro de segurança. |
| minPasswordLength | Número inteiro | O número mínimo de caracteres necessários para senhas de usuário. |
| minPasswordCharacters | Número inteiro | Número mínimo de caracteres alfabéticos necessários para senhas de usuário. |
| minPasswordNumerals | Número inteiro | Número mínimo de caracteres numéricos necessários nas senhas de usuário. |
| passwordLifetime | Número inteiro | Número de dias antes que um usuário seja solicitado a alterar sua senha. |
| graceLogins | Número inteiro | Número máximo de tolerâncias de logon permitidas após a expiração de uma senha. |
| maxRetries | Número inteiro | Número máximo de vezes que um usuário pode tentar fazer log-on sem sucesso no sistema antes de a conta ser bloqueada. |
| lockDuration | Número inteiro | Tempo pelo qual a conta de um usuário permanece bloqueada após ultrapassar o número máximo de tentativas de log-on. A unidade de medida é definida no parâmetro lockIntervalType. |
| lockIntervalType | Número inteiro | Tipo de duração do bloqueio (1 = horas, 2 = minutos e 3 = dias). |
| sessionTimeout | Número inteiro | Período limite de inatividade para uma sessão de usuário. A unidade de medida é definida no parâmetro timeoutIntervalType. |
| passwordHistoryCheckDepth | Número inteiro | Número de senhas anteriores a rastrear. Os usuários não têm permissão para reutilizar essas senhas rastreadas. |
| expirationNotice | Número inteiro | Número de dias para exibição de um aviso antes da expiração da senha. |
| accountTimeout | Número inteiro | Número de dias após o qual o status de uma conta é automaticamente alterado para inativo caso o usuário não tenha feito log-on (0 = nenhum ou nunca desativa automaticamente). |
| timeoutIntervalType | Número inteiro | Unidade de medida de sessionTimeout (1 = horas, 2 = minutos e 3 = dias). |
| pinTimeout | Número inteiro | Período máximo de tempo que um PIN permanece ativo antes de o PIN expirar. |
| pinTimeoutType | Número inteiro | Tipo de tempo limite do PIN (1 = horas, 2 = minutos e 3 = dias). |
| pinMaxResendAttempts | Número inteiro | Número de vezes que os usuários podem solicitar um PIN antes que o sistema os impeçam de solicitar PINs adicionais. |
| pinResendLockTimeout | Número inteiro | Período de bloqueio antes que os usuários possam solicitar um PIN após excederem o limite máximo de solicitação de PIN. |
| pinResendLockTimeoutType | Número inteiro | Tipo de tempo limite de bloqueio de reenvio de PIN (1 = horas, 2 = minutos e 3 = dias). |

**Saída.** Este método retorna um número inteiro. Se o método for bem-sucedido, o valor será o ID do parâmetro de segurança recém-criado. Se houver uma falha, a API emitirá uma exceção.

## Amostra

Exemplo de chamada C#

iSecParmID = accesscontrol.CreateSecurityParameter(sSessionToken, “secparmname”, “description”, 6, 2, 2, 10, 13, 7, 1, 1, 51, 11, 3, 41, 1);

Exemplo de solicitação

Veja a seguir um exemplo de solicitação e resposta SOAP 1.1. Os espaços reservados mostrados seriam substituídos por valores reais. SOAP 1.2 também é compatível.

POST /archer/ws/accesscontrol.asmx HTTP/1.1

Host: staging

Content-Type: text/xml; charset=utf-8

Content-Length: **length**

SOAPAction: "http://archer-tech.com/webservices/CreateSecurityParameter"

<?xml version="1.0" encoding="utf-8"?>

<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

* <soap:Body>
  + <CreateSecurityParameter xmlns="http://archer-tech.com/webservices/">
    - <sessionToken>**string**</sessionToken>
    - <name>**string**</name>
    - <description>**string**</description>
    - <minPasswordLength>**int**</minPasswordLength>
    - <minPasswordCharacters>**int**</minPasswordCharacters>
    - <minPasswordNumerals>**int**</minPasswordNumerals>
    - <passwordLifetime>**int**</passwordLifetime>
    - <graceLogins>**int**</graceLogins>
    - <maxRetries>**int**</maxRetries>
    - <lockDuration>**int**</lockDuration>
    - <lockIntervalType>**int**</lockIntervalType>
    - <sessionTimeout>**int**</sessionTimeout>
    - <passwordHistoryCheckDepth>**int**</passwordHistoryCheckDepth>
    - <expirationNotice>**int**</expirationNotice>
    - <accountTimeout>**int**</accountTimeout>
    - <timeoutIntervalType>**int**</timeoutIntervalType>
    - <pinTimeout>**int**</pinTimeout>
    - <pinTimeoutType>**int**</pinTimeoutType>
    - <pinMaxResendAttempts>**int**</pinMaxResendAttempts>
    - <pinResendLockTimeout>**int**</pinResendLockTimeout>
    - <pinResendLockTimeoutType>**int**</pinResendLockTimeoutType>
  + </CreateSecurityParameter>
* </soap:Body>

</soap:Envelope>

Exemplo de resposta

HTTP/1.1 200 OK

Content-Type: text/xml; charset=utf-8

Content-Length: **length**

<?xml version="1.0" encoding="utf-8"?>

<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

* <soap:Body>
  + <CreateSecurityParameterResponse xmlns="http://archer-tech.com/webservices/">
    - <CreateSecurityParameterResult>**int**</CreateSecurityParameterResult>
  + </CreateSecurityParameterResponse>
* </soap:Body>

</soap:Envelope>